(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 575 765 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
27.10.1999 Bulletin 1999/43

(51) Int Cl.[6]: **G06F 12/14**

(21) Application number: **93108406.5**

(22) Date of filing: **25.05.1993**

(54) **Secure file erasure**

Sichere Dateilöschung

Effacement de fichier sécurisé

(84) Designated Contracting States:
DE FR GB

(30) Priority: **23.06.1992 US 902607**

(43) Date of publication of application:
29.12.1993 Bulletin 1993/52

(73) Proprietor: **Hughes Electronics Corporation**
El Segundo, California 90245-0956 (US)

(72) Inventor: **Kung, Kenneth C .**
Cerritos, California 90701 (US)

(74) Representative: **Witte, Alexander, Dr.-Ing. et al**
Witte, Weller, Gahlert, Otten & Steil,
Patentanwälte,
Rotebühlstrasse 121
70178 Stuttgart (DE)

(56) References cited:
EP-A- 0 471 538

- **PATENT ABSTRACTS OF JAPAN vol. 013, no. 256 (P-884)14 June 1989 & JP-A-01 053 241 (BROTHER IND LTD) 1 March 1989**

EP 0 575 765 B1

Description

[0001] The present invention relates to a method of deleting a file stored on a permanent storage medium of a computer system.

[0002] Generally, the present invention relates to computer systems, and more particularly, to methods of deleting (erasing) files stored on permanent storage media of a computer system that eliminates the possibility of recovery of the data as a readable file by unauthorized persons.

[0003] A traditional method for deleting a file from permanent storage space (a hard disk, for example) is to delete the pointer contained in the file directory that points to the information block comprising the file. The actual contents of the information is left untouched. Using a utility program, the contents of every block of storage space can be scanned for sensitive information.

[0004] More particularly, although storage space is fed up for other uses, the file's data content is left untouched until the storage space is actually used for another file storage. This is inherently dangerous because the user believes the data is gone, yet a skilled intruder can use powerful utility tools to scan for these deleted files.

[0005] Another conventional method of file deletion requires a user to overwrite 0's and 1's over the entire data file as to remove any magnetic remnants of the removed information. This method is slow because the system must write 0's and 1's many times to ensure the stored information cannot be recovered.

[0006] Such a method, for example, is known from Patent Abstracts of Japan, Vol. 013, No. 256 (P-884) June 14, 1989. According to the disclosed method the directory area as well as the data area of the file to be deleted is overwritten by 0's, thus requiring a comparable high processing time.

[0007] Further, EP-A-0 471 538 discloses a data security system in which the disk controller incorporates a hardware encryption circuit, which encodes data passing from the host computer to the disk and decodes data passing in the reverse direction. Operation of the encryption circuit is controlled by a coded signal which is generated by means of a "key" which provides a multi-digit code. This document is not concerned with file erasure.

[0008] It is therefore an object of the present invention to provide a methode for deleting files stored on permanent storage media. It is a further object to provide for a file deletion method whereby files are permanently deleted without the possibility of recovery. It is a further object to provide for a file deletion method whereby files are deleted in a manner that does not permit recovery by a person other than the original user or someone authorized by the user, and thus permits recovery of the deleted file.

[0009] In order to provide for the above and other objectives and features, the present invention provides for a method wherein an encryption algorithm is used to encrypt the data in a stored file when deleting the file. The encryption algorithm, such as a Type I or Type II encryption algorithm employed in a Secure Data Network Protocol (SDNP) processor manufactured by the assignee of the present invention, may be employed during file erasure to eliminate the weaknesses mentioned with regard to the conventional file erasure methods. The SDNP processor includes an integrated circuit chip that incorporates a selected one of the NSA-developed encryption algorithms. The Type 1 algorithm allows encryption of files containing classified information, and has a level of encryption that permits the encrypted files to be transferred to others without risk of exposure of the data contained in the files. The Type II algorithm is similar to the Type I algorithm but has been developed for nonclassified but sensitive data.

[0010] In accordance with the present invention, when a user requests deletion of a stored file, the file is encrypted so that it is not readable. The erasure is performed by using the encryption algorithm so that the contents of the file cannot be retrieved by other users after the erasure. Both one way and two way file deletion may be employed. In the one way deletion mode, if the user does not expect to "undelete" the data, a one-way encryption algorithm is used to increase the speed of secure deletion of the file. In the two way deletion mode, the user has the option to undelete the file by decrypting the encrypted file or disk storage area where the deleted file is stored, as long as this operation is done before the storage space is used by other software programs.

[0011] When the secure deletion method of the present invention is used, no utility program can recover any information from the deleted file. To an intruder, the storage space is encrypted to look like random bits. Therefore, no information can be retrieved nor derived from the encrypted, deleted file.

[0012] The present invention provides an enhancement for the existing file deletion function of the operating system any computer system so that if a user wants to securely delete the contents of a particular file, the file will be unreadable by anyone else. Using the present file deletion scheme employing the encryption algorithm when deleting data files eliminates the vulnerability present in conventional file deletion methods. The present invention thus permits a user to erase files from a permanent storage space (a hard of floppy disk, for example) and in a manner that makes the file totally unreadable by others.

[0013] The present invention also comprises a method of processing a file stored on a permanent storage medium of a computer system that eliminate access to the file by unauthorized persons. The method comprises selecting a stored file, encrypting the stored file using a random key, and then deleting a file directory pointer to the data file. The random key is stored externally and is in possession of the authorized user of the computer system. To recover the data, the method restores the

file directory pointer to the data file, and decrypts the encrypted stored file using the same random, externally stored, key used to encrypt the file to permit access to the data contained in the stored file.

[0014] The various features and advantages of the present invention may be more readily understood with reference to the following detailed description taken in conjunction with the accompanying drawing, and in which the sole figure illustrates a method in accordance with the principles of the present invention that securely deletes a file stored on a storage medium of a computer system.

[0015] Referring to the drawing figure, it illustrates a secure file erasure method 10 in accordance with the principles of the present invention that securely and permanently deletes a file 20 stored on a storage medium 15 of a computer system 16. The computer system 16 includes a hard disk employed as the storage medium 15, and has a keyboard or mouse device (not shown) to provide inputs to the computer system 16. The computer system 16 includes an operating system that contains a conventional delete file command as one of its functions. The delete file command is employed to delete files 20 stored on the storage medium 15.

[0016] In accordance with the principles of the present invention, if a user of the computer system 16 desires to delete the file 20 stored on the storage medium 15, the user enters a delete file commend 11 by selecting from a menu on a computer screen (not shown) or by typing a delete file command sequence on the keyboard. A firmware processing routine in accordance with the principles of the present invention that is stored in a ROM or as an application program that runs on the computer system 10 intercepts the delete file command and prompts the user on the display screen 17 if a secure deletion of the stored file 20 is desired, illustrated by decision block 12. If no secure file deletion is desired, then the method 10 of the present invention proceeds to a normal delete file process 14. This normal delete file process may be a traditional file deletion process described in the Background section, wherein a pointer contained in the file directory of the storage medium 15 that points to the information blocks comprising the file 20 is deleted. In this situation, the actual contents of the information in the file 20 is left untouched.

[0017] If, however, a secure deletion of the file 20 is desired, then an encryption algorithm 13 is used to encrypt the file 20 whose contents is to be deleted. The encryption algorithm 13 may comprise a Type I or Type II algorithm employed in a Secure Data Network Protocol processor developed by the assignee of the present invention. This algorithm is incorporated in an integrated circuit chip that may be purchased from the National Security Administration (NSA). The chip is incorporated in a Secure Data Network Protocol (SDNP) processor manufactured by the assignee of the present invention, which may be employed for the purposes of encryption of the file 20. Once the file 20 has been encrypted by the encryption algorithm 13 the method proceeds to the normal deletion process step 14 which deletes the directory pointer.

[0018] The specifics of the encryption algorithm employed in the present method 10 are as follows. Both one way and two way file deletion modes 17, 18 may be employed using the encryption algorithm 13. In the one way deletion mode 17, wherein the user does not expect to "undelete" the data, a one-way encryption algorithm is used to increase the speed of secure deletion of the file 20. In the one way mode 17, the data in the file 20 is encrypted using a random external key 21, and then the key 21 is automatically destroyed 19 and cannot be used to recover the data. Consequently, without the key 21, the data cannot be decrypted and is thus unreadable by anyone.

[0019] In the two way mode 18, the data in the file 20 is encrypted using the random key 21, but the key 21 is not destroyed 19 and may be used by the user to recover the data. The key 21 is stored or retained by the user in a secure location external to the computer system 16. In the two way deletion mode 18, the user has the option to undelete the file 20 by restoring the directory pointer 23 decrypting 24 the encrypted file 20 or disk storage area where the deleted file 20 is stored, as long as this operation is done before the storage space is used by other software programs. Consequently, the data cannot be decrypted and is thus unreadable by anyone without the key 21. If the secure file deletion method 10 of the present invention is used, no utility program can recover any information from the deleted file 20. To an intruder, the storage space is encrypted to look like random bits. Therefore, no information can be retrieved nor derived from the encrypted, deleted file 20.

[0020] In summary, then, the method 10 of present invention comprises processing the file 20 stored on the permanent storage medium 15 of the computer system 16 which eliminate access to the file by unauthorized persons. The method includes selecting the stored file 20 and entering a delete command 11, encrypting the stored file 20 using a random key 21 and by operating on the file 20 with the encryption algorithm 13, and then deleting 14 a file directory pointer to the file 20. To recover the file 14, the method 10 restores the file directory pointer 23 to the file 20, and decrypts 24 the encrypted stored file 20 using the random key 21 to permit access to the data contained in the stored file 20.

[0021] The present invention thus permits a user to erase files 20 from a permanent storage space and in a manner that makes the file totally unreadable by others. The erasure is performed by using the encryption algorithm so that the contents of the file 20 cannot be retrieved after the erasure. This is different from the traditional file erasure method discussed in the Background section where only the file directory information is deleted or the pointer to the file 20 is deleted. In this conventional method storage space is freed up for other uses, the file's data content is left untouched until the storage

space is actually used for storage of another file. This is inherently dangerous because the user believes the data is gone, yet a skilled intruder can use powerful utility tools to scan for these deleted files. By using the present file erasure method employing an encryption algorithm when deleting files 20 eliminates this vulnerability.

[0022] Thus there has been described new and improved methods of deleting (erasing) files stored on permanent storage media of a computer system that eliminates the possibility of recovery of the data as a readable file by unauthorized persons.

Claims

1. A method (10) of deleting a file (20) stored on a permanent storage medium (15) of a computer system (16), said method (10) comprising the steps of:

   selecting responsive to a user command, (11) a stored file (20) for deletion; and
   deleting (14) a file directory pointer to the file (20);
   the method being characterized by further comprising, at a time prior to deleting the directory pointer, the step of encrypting (13) the stored file (20) using a random key (21).

2. The method (10) of Claim 1 further characterized by the step of:

   after encrypting (13) the stored file (20) using the random key (21), destroying (19) the random key (21).

3. The method (10) of Claim 1 further characterized by the steps of:

   at a time prior to overwriting of storage locations of the encrypted file (20), restoring (23) the file directory pointer to the file (20); and
   decrypting (24) the encrypted stored file (20) using the random key (21) to permit access to the stored file (20).

Patentansprüche

1. Verfahren (10) zum Löschen einer in einem Permanentspeichermedium (15) eines Computersystems (16) gespeicherten Datei (20), wobei das Verfahren (10) die Schritte aufweist:

   Auswahl (11) einer zu löschenden gespeicherten Datei (20) durch einen Benutzerbefehl, und Zerstören (14) eines auf die Datei (20) weisenden Dateiverzeichnis-Zeigers;
   wobei das Verfahren dadurch gekennzeichnet ist, daß es außerdem, zu einem Zeitpunkt vor dem Zerstören des Verzeichnis-Zeigers, den Schritt umfaßt,
   die gespeicherte Datei (20) unter Verwendung eines Zufallsschlüssels (21) zu verschlüsseln (13).

2. Verfahren (10) nach Anspruch 1, zusätzlich gekennzeichnet durch den Schritt, nach dem unter Verwendung des Zufallsschlüssels (21) erfolgten Verschlüsseln (13) der gespeicherten Datei (20) den Zufallsschlüssel (21) zu zerstören (19).

3. Verfahren (10) nach Anspruch 1, weiter gekennzeichnet durch die Schritte:

   Wiederherstellen (23) des auf die Datei (20) weisenden Dateiverzeichnis-Zeigers zu einem Zeitpunkt vor dem Überschreiben von Speicherstellen der verschlüsselten Datei (20); und Entschlüsseln (24) der verschlüsselten gespeicherten Datei (20) unter Verwendung des Zufallsschlüssels (21), um einen Zugriff auf die gespeicherte Datei (20) zu ermöglichen.

Revendications

1. Procédé (10) d'effacement d'un fichier (20) stocké sur un support (15) de stockage permanent d'un système (16) informatique, ledit procédé (10) comprenant les étapes consistant à :

   sélectionner (11), en réponse à un ordre de l'utilisateur, un fichier stocké (20) pour son effacement ; et
   effacer (14) un pointeur d'un répertoire de fichiers pointant sur le fichier (20) ;
   le procédé étant caractérisé par le fait qu'il comprend en outre, à un instant antérieur à l'effacement du pointeur de répertoire, l'étape consistant à :
   encrypter (13) le fichier stocké (20) en utilisant une clé aléatoire (21).

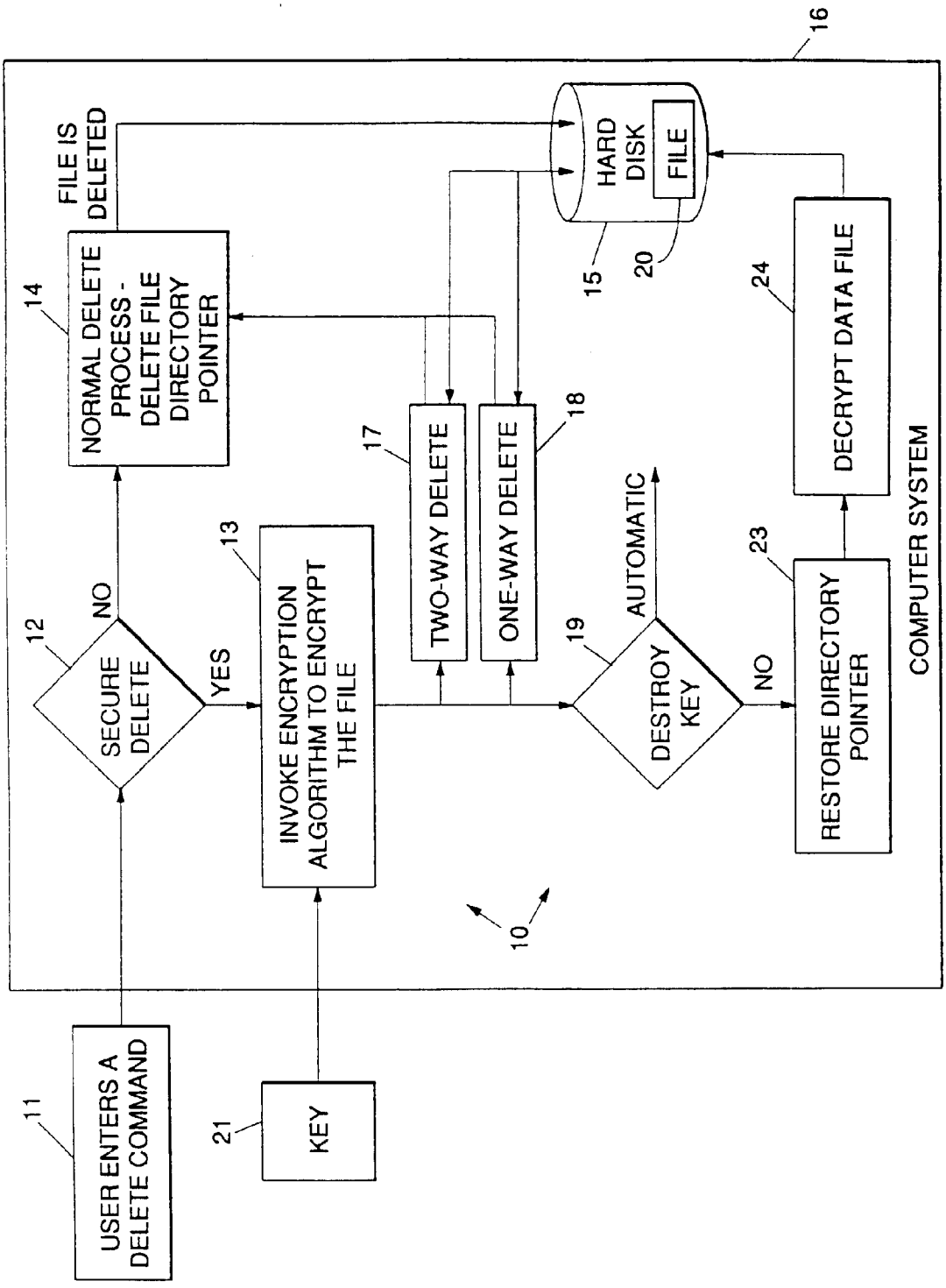
2. Procédé (10) selon la revendication 1, caractérisé en outre par l'étape consistant à :

   après avoir encrypté (13) le fichier stocké (20) à l'aide de la clé aléatoire (21), à détruire (19) la clé aléatoire (21) .

3. Procédé (10) selon la revendication 1, caractérisé en outre par les étapes consistant à :

   à un instant antérieur à la réécriture d'emplacements de stockage du fichier encrypté (20), rétablir (23) le pointeur de répertoire de fichiers

pointant sur le fichier (20) ; et
décrypter (24) le fichier stocké encrypté (20) à l'aide de la clé aléatoire (21) pour permettre un accès au fichier stocké (20).


16
FILE IS DELETED
HARD DISK
FILE
15
20
14
NORMAL DELETE PROCESS - DELETE FILE DIRECTORY POINTER
17
TWO-WAY DELETE
18
ONE-WAY DELETE
24
DECRYPT DATA FILE
12
NO
SECURE DELETE
YES
13
INVOKE ENCRYPTION ALGORITHM TO ENCRYPT THE FILE
19
AUTOMATIC
DESTROY KEY
NO
23
RESTORE DIRECTORY POINTER
COMPUTER SYSTEM
10
11
USER ENTERS A DELETE COMMAND
21
KEY